

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and a second execution environment, comprising the steps of:

accepting encrypted user input from a user input device intended for either said secured execution environment or said second execution environment, ~~wherein the encrypted user input does not contain an explicit indication of an intended execution environment;~~

decrypting said encrypted user input;

determining, ~~based on said decrypted user input,~~ a graphical user element that has focus from among at least one graphical user elements;

determining whether a process that owns the graphical user element is in the secured execution environment or in the second execution environment;

determining, based on whether the process that owns the graphical user element is in the secured execution environment or in the second execution environment, whether said decrypted user input is intended for said secured execution environment;

if said decrypted user input is not intended for said secured execution environment, transferring said decrypted user input to said second execution environment;

if said decrypted user input is intended for said secured execution environment, determining a specific destination entity within said secured execution environment for said decrypted user input, and transferring said decrypted user input to said specific destination entity;

accepting output from a specific source entity within said secured execution environment and not within said second execution environment; and

securely transferring said output to an output device.

2. (Canceled)

3. (Original) The method of claim 1, where said step of accepting user input from a user input device comprises establishing a secure communications channel with said user input.

4. (Original) The method of claim 1, where said step of accepting user input from a user input device comprises verifying said user input.

5. – 6. (Canceled)

7. (Previously presented) The method of claim 1, where said step of transferring said decrypted user input to said specific destination entity comprises:
interpreting said decrypted user input.

8. (Canceled)

9. (Previously presented) The method of claim 1, where said step of securely transferring said output to said output device comprises:
encrypting said output data.

10. (Previously presented) The method of claim 1, where said step of securely transferring said output to said output device comprises:
transferring said output to a curtailed memory.

11. (Canceled)

12. (Currently Amended) The method of claim [[11]] 1, where said output contains a data portion, and where said step of securely transferring said output to said output device comprises:
encrypting said data portion of said output.

13. (Currently Amended) The method of claim [[11]] 1, where said step of securely transferring said output to said output device comprises:
transferring said output to a curtained memory.

14. (Currently Amended) A computer-readable storage medium containing computer executable instructions to provide a secure user interface to a secured execution environment on a system comprising said secured execution environment and a second execution environment, the computer-executable instructions to perform acts comprising:

accepting encrypted user input from a user input device intended for either said secured execution environment or said second execution environment ~~wherein the encrypted user input does not contain an explicit indication of an intended execution environment;~~

decrypting said encrypted user input;

determining, ~~based on said decrypted user input,~~ a graphical user element that has focus from among at least one graphical user elements;

determining whether a process that owns the graphical user element is in the secured execution environment or in the second execution environment;

determining, based on whether the process that owns the graphical user element is in the secured execution environment or in the second execution environment, whether said decrypted user input is intended for said secured execution environment; ~~and~~

if said decrypted user input is not intended for said secured execution environment, transferring said decrypted user input to said second execution environment;

if said decrypted user input is intended for said secured execution environment, determining a specific destination entity within said secured execution environment for said decrypted user input, and transferring said decrypted user input to said specific destination entity;

accepting output from a specific source entity within said secured execution environment and not within said second execution environment; and

securely transferring said output to an output device.

15. (Canceled)

16. (Previously presented) The computer-readable storage medium of claim 14, where said accepting user input from a user input device comprises establishing a secure communications channel with said user input.

17. (Previously presented) The computer-readable storage medium of claim 14, where said accepting user input from a user input device comprises verifying said user input.

18. – 19. (Canceled)

20. (Currently Amended) The computer-readable storage medium of claim ~~[[18]]~~ 14, where said transferring said user input to said specific destination entity comprises:
interpreting said user input.

21. (Canceled)

22. (Currently Amended) The computer-readable storage medium of claim ~~[[21]]~~ 14, where said output contains a data portion, and where said securely transferring said output to said output device comprises:
encrypting said data portion of said output.

23. (Currently Amended) The computer-readable storage medium of claim ~~[[21]]~~ 14, where said securely transferring said output to said output device comprises:
transferring said output to a curtailed memory.

24. – 26. (Canceled)

27. (Currently Amended) A trusted user interface engine for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and a second execution environment, comprising:

an input trusted service provider accepting encrypted user input from a user input device and decrypting said encrypted user input, operably connected to said user device;

a trusted input manager for determining, ~~based on said decrypted user input, wherein the decrypted user input does not contain an explicit indication of an intended execution environment,~~ a graphical user element that has focus from among at least one graphical user elements, determining whether a process that owns the graphical user element is in the secured execution environment or in the second execution environment, and, determining, based on whether the process that owns the graphical user element is in the secured execution environment or in the second execution environment, whether said decrypted user input is intended for said secured execution environment and,

if said decrypted user input is not intended for said secured execution environment, transferring said decrypted user input to said second execution environment, and

if said decrypted user input is intended for said secured execution environment, determining a specific destination entity within said secured execution environment for said decrypted user input, and transferring said decrypted user input to said specific destination entity; and

a trusted output manager for accepting output from a specific source entity within said secured execution environment and not within said second execution environment and securely transferring said output to an output device.

28. (Canceled)

29. (Original) The trusted user interface engine of claim 27, where said input trusted service provider establishes a secure communications channel with said user input.

30. (Original) The trusted user interface engine of claim 27, where said input trusted service provider verifies said user input.

DOCKET NO.: MSFT-2817/301134.01
Application No.: 10/693,407
Office Action Dated: May 29, 2008

**PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116**

31. – 32. (Canceled)

33. (Original) The trusted user interface engine of claim 31, where said trusted input manager interprets said user input for said specific destination entity.

34. (Canceled)

35. (Currently Amended) The trusted user interface engine of claim ~~[[34]]~~ 27, where said output contains a data portion, and where said trusted output manager encrypts said data portion of said output.

36. (Currently Amended) The trusted user interface engine of claim ~~[[34]]~~ 27, where said trusted output manager transfers said output to a curtained memory.

37. – 40. (Canceled)